REMARKS

This response is submitted along with a request for a one-month extension of time and the requisite fee. Claims 1-19 were pending and claims 1-19 were rejected. Claim 11 has been amended and claims 1-19 remain pending.

Claims 1-19 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2002/0012432 ("England"). Applicants respectfully traverse the rejection and request withdrawal of the rejection.

England generally describes a system for enforcing rights to protected digital content in which the digital content may be obtained over a public network such as the Internet. The rights are determined by a license, and a user's computing device 14 may obtain a license from a license server via the Internet. Similarly, the user's computing device 14 may obtain encrypted content from a content server via the Internet. A digital rights management (DRM) system on the user's computing device 14 permits decryption of the protected content only if the user's computing device 14 also has obtained a license to use the content from the license server. The DRM system of England utilizes a "black box", which is obtained by the user's computing device 14 from a black box server.

On the other hand, the claims of the present application are directed to a system that, in some implementations, may be less complex than the England system in that it may not require use of a license server, for example. Implementations of the claimed subject matter may be more appropriate for distributions and control of content within an organization as opposed to distributions over a public network. (Of course, in some implementations of the claimed subject matter, distribution may also occur via a public network such as the Internet.) As a result of the differences between the system of England and the claimed subject matter, England does not disclose the claimed combination of elements, as will be discussed in more detail below.

Rejection Under 35 U.S.C. §102(e)

It is well settled that a rejection under 35 U.S.C. §102(e) requires the presence of a "single prior art disclosure of each and every element of a claimed invention." *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747 (Fed. Cir. 1987); *see also, MPEP* §2131 ("A claim is anticipated only if each and every element as set forth in the claim is found" quoting *Verdegall Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)).

To establish anticipation, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Here, the Final Office Action does not establish that England discloses every element of each claim.

Claim 1

Claim 1 is directed to a digital information security system. The system comprises, *inter alia*, "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal," and "a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication."

The Final Office Action failed to establish that England discloses all the elements of claim 1. For example, the Final Office Action failed to establish that England discloses "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal," in combination with "a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication."

England describes a system for distributing encrypted digital content and allowing persons with rights to view the digital content to decrypt the content. The system includes an authoring tool 18, a content server, a license server, a black box server, and a user's computing device 14. The authoring tool 18 is used by a content owner to package a piece of digital content for use in the system. *See England* at par. 0048. The authoring tool 18 creates packages that include encrypted content. The content server downloads a package to a user's computing device 14 in response to a request from the user. *See England* at par.

0077, Fig. 1. The user's computing device 14 includes a rendering application that conditionally renders digital content and a digital rights management (DRM) system. *See id.* at par. 0120, Fig. 4. When a user attempts to render encrypted content downloaded from the content server, the rendering application invokes the DRM system. *See id.* at par. 0120. The DRM system checks whether the user has a license to render the downloaded content. If the user does not, the DRM system may download a license from the license server. *See id.* at par. 0011, Fig. 1. The license may include a decryption key to enable the user computing device to decrypt the digital content. *See id.* at par. 0012. The decryption key in the license is itself encrypted. *See id.* at par. 0017. A "black box" in the DRM system includes a public/private key pair. *See id.* at par. 0016. The license server uses the public key from the black box to encrypt the decryption key in the license, and the DRM system on the user's computing device 14 uses the private key from the black box to decrypt the decryption key in the license. *See id.* at par. 0017. The "black box" as well its public/private key pair is downloaded from the black box server to the user's computing device 14. *See id.* at pars. 0016, 0178.

As best can be understood, the Final Office Action appears to assert that England discloses "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal," as recited in claim 1, for two alternate reasons: (1) England discloses the authoring tool 18, and (2) England discloses the user's computing device 14. But England does not disclose or suggest that the authoring tool 18 or the user's computing device 14 includes a "user application tool being structured to create a unique user key using unique system information of the user terminal," and further that there is "a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication."

With regard to the authoring tool 18, although England explains that the authoring tool 18 uses keys, England discloses that the authoring tool 18 does not create the keys it uses. Namely, England discloses that the keys used by the authoring tool 18 are received by the authoring tool 18:

> The authoring tool 18 is a dynamic authoring tool 18 that receives input parameters ... the input parameters are embodied in the form of a dictionary 28, as shown, where the dictionary 28 includes such parameters as ... the encryption/decryption key to be employed.

England at pars. 0062, 0065 (emphasis added). Thus, it cannot be said that England discloses that the authoring tool 18 creates the encryption/decryption keys.

Moreover, even if England did disclose that the authoring tool 18 created "a unique user key using unique system information of the user terminal" (which is not admitted), England does not appear to disclose that a server receives such a user key from the authoring tool 18, stores the user key, and then uses the key to authenticate a user. Thus, if the Final Office Action asserts that the authoring tool 18 corresponds to the recited user application tool, the Final Office Action failed to establish that England discloses "a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication."

With regard to the user's computing device 14 of England, England explains that the user's computing device 14 uses keys, and that these keys are received by the user's computing device 14 from a license server and a black box server. *See id.* at pars. 0011, 0012, 0176, 0178. Thus, England makes clear that these keys are not created by something installed on the user's computing device 14. Because England explains that the various keys used by the user's computing device 14 are received from the license server and the black box server, it cannot be said that the description of the user's computing device 14 is a disclosure of "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal."

Additionally, the Final Office Action asserts that "every CPU is capable of performing cryptographic functions, such as signing, encrypting, decrypting and authenticating. A CPU manufacturer equips a CPU with a pair of public and private keys that is unique to the CPU." *Final Office Action* at pp. 2-3. This discussion of CPU's is not disclosed in England, but it appears to come from somewhere outside of England. Moreover, England never describes the use of keys provided by a CPU manufacturer. Thus, it is unclear

how this can be used to support the assertion that England shows "[t]he identical invention ... in as complete detail as is contained in the ... claim." *Richardson*, 9 U.S.P.Q.2d at 1920 (emphasis added); MPEP §2131. A rejection under 35 U.S.C. §102(e) requires the presence of a "single prior art disclosure of each and every element of a claimed invention." *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747 (Fed. Cir. 1987) (emphasis added). Further, if the Final Office Action is alleging that this information is somehow inherent in England, Applicants respectfully traverse that assertion.

For the sake of argument, even if it were true that a CPU manufacturer equips every CPU with a pair of public and private keys, which is not admitted, England does not disclose that such keys are utilized in its system. For instance, England discloses that the keys used by the authoring tool 18 are received by the authoring tool 18:

> The authoring tool 18 is a dynamic authoring tool 18 that receives input parameters ... the input parameters are embodied in the form of a dictionary 28, as shown, where the dictionary 28 includes such parameters as ... the encryption/decryption key to be employed.

England at pars. 0062, 0065 (emphasis added). Thus, it cannot be said that England discloses that the encryption/decryption keys used by the authoring tool 18 are a pair of public and private keys that were equipped in a CPU of the authoring tool 18 by a CPU manufacturer. Similarly, England explains that the keys used by the user's computing device 14 are received from the license server and the black box server. Thus, it cannot be said that England discloses that the keys used by the user's computing device 14 are a pair of public and private keys that were equipped in a CPU of the user's computing device 14 by a CPU manufacturer.

Next, the Final Office Action states that "the distinction as to location of key creation is not relevant." *Final Office Action* at p. 3. Thus, it appears that the Final Office Action is essentially ignoring the claim language "a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal," in arguing that England anticipates claim 1. But it is improper to ignore claim limitations when determining whether a reference anticipates. *See MPEP* §2131. To establish anticipation, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). *See also, MPEP* §2106 ("[W]hen evaluating the scope of a claim, every limitation in the claim must be considered. Office personnel may not

dissect a claimed invention into discreet elements and then evaluate the elements in isolation. Instead, the claim as a whole must be considered.") (underlining in original); *Diamond v. Diehr*, 209 U.S.P.Q. 1, 9 (1981)("'In determining the eligibility of respondents' claimed process for patent protection under 101, their claims must be considered as a whole. It is inappropriate to dissect the claims into old and new elements and then to ignore the presence of the old elements in the analysis.'").

At least for the reasons discussed above, the Final Office Action failed to establish that England shows, "[t]he identical invention ... in as complete detail as is contained in the ... claim." *Richardson*, 9 U.S.P.Q.2d at 1920 (emphasis added); MPEP §2131. Thus, the Final Office Action failed to establish that England anticipates claim 1.

Claim 6

Claim 6 is directed to a digital information security method. The method comprises, *inter alia*, "reading a first unique user key created using unique system information of a user terminal when a server is accessed by a user," "comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user," "encrypting a file uploaded by the authorized user using a preset encryption key, and storing the encrypted file as digital information," "encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information," and "downloading the encrypted decoding key along with the associated digital information in response to a digital information download request of the authorized user."

The Office Action failed to establish that England discloses all the elements of claim 6. For example, the Office Action failed to establish that England discloses "reading a first unique user key created using unique system information of a user terminal when a server is accessed by a user," "comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user," and "encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information."

England explains that the license downloaded to a user's computing device 14 includes a decryption key for decrypting content. This decryption key is itself encrypted using a public key from a black box. England explains that the user's computing device 14

transmits the black box public key to the license server. *See* England at pars. 0146, 0147. But England does not disclose or suggest that the license server uses the black box public key to authenticate the user. Thus, England does not disclose "reading a first unique user key created using unique system information of a user terminal when a server is accessed by a user," "comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user," and "encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information."

Moreover, with regard to the user's computing device 14, although England explains that encrypted content is downloaded to the user's computing device 14, England does not appear to disclose files being uploaded from the user's computing device 14.

With regard to the authoring tool 18, England explains that the authoring tool 18 encrypts content. Thus, England does not disclose that the authoring tool 18 uploads content for it to be encrypted. Additionally, England does not explain how the content is provided to the authoring tool 18. Thus, the description provided by England of the authoring tool 18 is not a disclosure of "comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user," "encrypting a file uploaded by the authorized user using a preset encryption key, and storing the encrypted file as digital information."

At least for these reasons, the Final Office Action failed to establish that England anticipates claim 6.

Claim 10

Claim 10 is directed to a digital information security method. The method comprises, *inter alia*, "creating a unique user key at a user terminal using unique system information of the user terminal."

The Office Action failed to establish that England discloses all the elements of claim 10. For example, the Office Action failed to establish that England discloses "creating a unique user key at a user terminal using unique system information of the user terminal" at least for reasons similar to those discussed above with respect to claim 1.

Claim 11

Claim 11 has been amended to place the claim in better form for appeal. Entry of the amendment is respectfully requested. For instance, claim 11 has been amended to indicated that the "key management service module" is not required to be installed in a user system. The detailed description of the present application indicates that, in one embodiment, the key management service module may be part of a document management system or a knowledge management system separate from a user terminal. *See Specification* at pars. 0078, 0079; Fig. 6. Additionally, claim 11 has been amended to remove the phrase "the encrypted download file encrypted using the unique user ID," which was added to claim 11 by the previous amendment mailed on June 9, 2005.

Claim 11 is directed to a digital information security system. The system comprises, *inter alia*, "a document management service gateway structured to create a document key for a file when the file is uploaded from the user, store the created document key, and encrypt a corresponding file using the created document key." England does not disclose this element.

England explains that the authoring tool 18 receives content and also receives encryption/decryption keys. The authoring tool 18 encrypts the content with a received encryption/decryption key. England does not disclose that the authoring tool 18 creates the encryption/decryption key. Rather, England explains that the authoring tool 18 receives the encryption/decryption key, but does not explain how it is created. Thus, England does not disclose "a document management service gateway structured to create a document key for a file when the file is uploaded from the user, store the created document key, and encrypt a corresponding file using the created document key."

At least for this reason, the Final Office Action failed to establish that England anticipates claim 11.

Claim 16

Claim 16 is directed to a digital information security method related to a file that has been uploaded by a user. The method comprises, *inter alia*, "transmitting by the web server information on the uploaded file to the document management service gateway," "reading by the document management service gateway the uploaded file by accessing a position where the file is actually uploaded from the server, using the information on the

uploaded file," "creating a document key for the read file in a predetermined decoding method, and storing the created document key along with the corresponding file information," "encrypting the file using the created document key," "storing the encrypted file in a predetermined folder," and "informing the web server that processing of the uploaded file is completed."

England describes an authoring tool and a content server. *See England* at Fig. 1. The authoring tool encrypts content and the content server distributes the encrypted content. *See id.* at par. 0048, 0076. It appears that the authoring tool 18 is part of the content server. Namely, England explains that the authoring tool 18 encrypts content and also explains that the content server encrypts content. *See id.* at pars. 0010, 0048.

England does not disclose the combination of elements recited in claim 16. For example, England does not disclose "reading by the document management service gateway the uploaded file by accessing a position where the file is actually uploaded from the server, using the information on the uploaded file," "storing the encrypted file in a predetermined folder," and "informing the web server that processing of the uploaded file is completed." Accordingly, the Office Action failed to establish that England discloses all the elements of claim 16.

Other Claims

Claims 2-5 depend from claim 1. It is respectfully submitted that claims 2-5 are allowable for the same reasons as claim 1, as well as for additional reasons.

Claims 7-9 depend from claim 6. Applicants respectfully submit that claims 7-9 are allowable for the same reasons as claim 6, as well as for additional reasons.

Claims 12-15 depend from claim 11. It is respectfully submitted that claims 12-15 are allowable for the same reasons as claim 11, as well as for additional reasons.

Claims 17-19 depend from claim 16. Applicants respectfully submit that claims 17-19 are allowable for the same reasons as claim 16, as well as for additional reasons.

Conclusion

In view of the above, Applicants believes that claims 1-19 are allowable and that the pending application is in condition for allowance.

Dated: December 15, 2005

Respectfully submitted,

By _____
Gregory E. Stanton
Registration No.: 45,127
MARSHALL, GERSTEIN & BORUN LLP
233 S. Wacker Drive, Suite 6300
Sears Tower
Chicago, Illinois 60606-6357
(312) 474-6300
Attorney for Applicants